UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Digital Devices copied onto a Seagate Barracuda Drive currently located at the evidence vault at 2121 SW 4th Ave, Suite 301, Portland, Oregon 97201	Case No. 3:25-mc-39

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Digital Devices copied onto a Seagate Barracuda Drive currently located at the evidence vault at 2121 SW 4th Ave, Suite 301, Portland, Oregon 97201, as described in Attachment A hereto,

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 641	THEFT OF GOVERNMENT FUNDS
18 U.S.C. § 1343	WIRE FRAUD

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Christopher Miller, Special Agent, VA OIG
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 12:17 ~~x~~.m./p.m. *(specify reliable electronic means)*.

Date: January 14, 2025

Youlee Yim You
Judge's signature

City and state: Portland, Oregon

YOULEE YIM YOU, United States Magistrate Judge
Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF CHRISTOPHER MILLER

Affidavit in Support of an Application for a Search Warrant

I, Christopher Miller, being duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Department of Veterans Affairs ("VA"), Office of Inspector General ("OIG"). I have held this position since October 2014. I was previously a Special Agent with the U.S. Secret Service from July 2006 to October 2014. My current assignment is to the Northwest Field Office in the Portland, Oregon Resident Agency. My training and experience include criminal law and procedure training at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia and at the U.S. Secret Service Academy in Beltsville, Maryland.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of the following devices: MacBook Air (FVHY9DPTJ1WK), MacBook Pro (serial C02NV957G3QD), MacBook Pro (serial ND2K2H2WJH), MacBook Pro (serial NMVT7XK9XK), MacBook Pro (serial PWYWX2HJP9), HP Pavilion (serial SCG-10174YS), and iPhone 14 Pro (serial LJ6TH5L7) (collectively referred to as the "**Subject Devices**"). The Subject Devices were imaged and copied onto a Seagate Barracuda Drive (serial W1F54ND8) (the "Drive"), which is currently stored, in law enforcement possession at the VA OIG Portland, Oregon evidence vault located at 2121 SW 4th Avenue, Suite 301, Portland, Oregon 97201, as described in Attachment A hereto. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence of violations of Title 18, United States Code, Sections 641 (Theft of Government Funds) and 1343 (Wire Fraud).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communication with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. *Title 18, United States Code, Section 641* makes it unlawful for any person to embezzle, steal, purloin, or knowingly convert to his use or the use of another, or without authority, sell, convey or dispose of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or for any person to receive, conceal, or retain the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted.

5. *Title 18, United States Code, Section 1343* makes it unlawful for any person, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, to transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

Statement of Probable Cause

A. Background on Investigation

6. The VA OIG was investigating whether PDX CODE GUILD and its owner and operator, Sheri Dover, were engaged in a scheme to fraudulently obtain education benefits paid by the United States on behalf of eligible veterans under VA programs, including the Post-9/11 GI Bill.

7. On December 2, 2022, I applied for and received a warrant to search the premises of PDX CODE GUILD at 407 NE 12th Avenue, Portland, Oregon, for evidence of violations of 18 U.S.C. § 641 and 18 U.S.C. § 1343, from United States Magistrate Judge Andrew D. Hallman (case no. 3:22-mc-01124). The application in support of that warrant, the accompanying affidavit and the search warrant are incorporated by reference into this affidavit. I have attached a copy of my affidavit in support of that warrant as **Exhibit 1** to this affidavit.

8. As detailed in Exhibit 1, I had probable cause to believe that the owner and operator of PDX Code Guild, Sheri Dover, had submitted materials to the VA falsely and fraudulently stating that PDX CODE GUILD met VA rules on the percentage of VA-supported students in PDX CODE GUILD's classes in order to receive VA educational payments.

9. On December 7, 2022, pursuant to the search warrant, federal agents from the VA OIG executed a search of the business offices of PDX CODE GUILD. During the search, agents imaged and copied the **Subject Devices** onto the Drive. The physical **Subject Devices** were left at the business offices of the PDX CODE GUILD and returned to the control of PDX CODE GUILD after being imaged.

10. After the **Subject Devices** were imaged onto the Drive, the **Subject Devices** were copied from the Drive onto evidence servers of the VA OIG and the Drive was stored at the VA OIG Portland, Oregon evidence vault.

11. The **Subject Devices** as uploaded from the Drive onto VA OIG evidence servers will be made available for review by VA OIG investigators. The evidence servers may be outside of the District of Oregon. Pursuant to this search warrant, agents will review the images of the **Subject Devices** as stored on VA OIG evidence servers, which are the same as the images of the **Subject Devices** as stored on the Drive.

12. Agents also seized physical evidence from the offices of PDX CODE GUILD. A search warrant return was provided to the Court and filed by the clerk's office on December 12, 2022.

13. A review of the **Subject Devices** showed PDX CODE GUILD consistently recorded incorrect data regarding its compliance with the percentage of VA supported students enrolled in its classes in violation of VA rules.

14. For instance, the 4/27/2020 Node and React course was documented by two different sets: six VA-supported students and one non-supported students and five VA-supported students and two non-supported students. A review of the final class attendance roster and student files revealed seven students; all should have been classified as VA-supported under the VA rules. Under VA rules, a class made up entirely of VA-supported students would not have received the VA educational assistance payments that PDX CODE GUILD received for the 4/27/2020 Node and React course.

15. Additionally, non-veteran student files identified that Dover kept purposely incorrect student files which showed tuition totals which were not paid. For instance, one

student's 4/27/2020 Node and React enrollment agreement listed a course cost of $10,500. No discounts or scholarships were noted. However, that student was a PDX CODE GUILD employee and self-reported to investigators that she attended the course for free, which meant that she should have been counted as a VA-supported student for PDX CODE GUILD reporting purposes.

16. A review of the physical evidence seized during execution of the search warrant also showed that Dover was charging non-veterans lower tuition rates than students receiving VA educational benefits and not documenting it in student files.

17. Student files from 2017 to 2020 were reviewed for admissions criteria, including veteran status, tuition cost, and the application of discounts and/or scholarships. Overall, the files showed non-veteran students were disproportionately awarded discounts. The discounts included those identified in PDX CODE GUILD course catalogs, such as diversity and income based scholarships, and discounts not reported in the catalogs, such as self-pay or cash discounts. The discounts ranged in amount for each student and from year to year. For instance, one non-veteran student attended a course in October 2019 with course tuition listed as $16,500. He was awarded an Income based discount with tuition listed as $8,500. The student listed his salary as $88,000 and stated he might be unemployed in the future.

18. Of note, PDX CODE GUILD's course catalog identified the following criteria for income or "needs based discounts": To qualify for a discount, a student must apply by submitting an essay that describes their economic need to a discount and how they plan to use the education and must show documentation that their yearly earnings fall below 3x the federal poverty guidelines and they must have less than half the federal poverty guidelines in savings.

19. Under the 2019 federal poverty guidelines, the 300% poverty guidelines for a two-person household residing in Oregon was $50,730. Therefore, the student referenced above with a salary of $88,000 exceeded the poverty guidelines. Further, the student did not provide documentation of his yearly earnings or state that he had less than half of his federal poverty guideline in savings.

20. On August 6, 2024, defendant Sheri Dover was charged in an indictment in case number 3:24-cr-00303-AN with five counts of wire fraud, in violation of 18 U.S.C. § 1343, and one count of theft of government funds, in violation of 18 U.S.C. § 641. Defendant is on release pending trial. Trial is currently scheduled for March 4, 2025.

Continued Need to Search the Subject Devices

21. Under the premises warrant, the VA OIG had to perform an initial search of the **Subject Devices** within 120 days of the execution of the warrant (*i.e.*, by or on April 11, 2023). An initial search of the **Subject Devices** found information responsive to the premises warrant.

22. Under the premises warrant, VA OIG had to complete its review of the **Subject Devices** within 180 days of the date of execution of the warrant (*i.e.*, by or on June 10, 2023). Based on the expected course of the prosecution, VA OIG ceased its review of the **Subject Devices** and did not conduct any further review of the Device after the 180-day period and did not seek an extension of the examination period.

23. VA OIG had performed a preliminary review of the **Subject Devices** at the time its review of the **Subject Devices** ceased due to the status of the prosecution. However, the course of the prosecution has since changed, and I am seeking a new warrant so VA OIG agents can continue their efforts to finish the review of the **Subject Devices** that was not completed within the timeframe of the original warrant.

24. The **Subject Devices** as imaged and copied on the Drive have been in VA OIG custody since being copied at PDX CODE GUILD's offices on December 7, 2022. I know from my training and experience and my knowledge of this investigation that the **Subject Devices** as stored on the Drive have been securely stored at VA OIG in a way that their contents are, to the extent material to this investigation, in the same state as they were in when the **Subject Devices** were first copied on the Drive. All of the data that was on the **Subject Devices** when first imaged and copied are still on the Drive. I also know that the lapse of time has not impacted the initial probable cause to search the **Subject Devices** under the warrant in matter 3:22-mc-01124 because the information copied from the **Subject Devices** has, in essence, been frozen in time while in VA OIG custody.

25. Based on the evidence of criminal conduct found on the digital devices imaged on the Device and the probable cause for the initial premises search warrant, I have probable cause to believe that evidence as described in Attachment B will be found on the **Subject Devices**. Therefore, I submit this application for a search warrant of the **Subject Devices**.

Search and Seizure of Computers and Computer Storage Media

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time.

27. There is probable cause to believe that things that were once stored on the **Subject Devices** will still be stored there because, based on my knowledge, training, and experience, I know:

a. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes

described on the warrant but also forensic evidence that establishes how the **Subject Devices** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the **Subject Devices** because, based on my knowledge, training, and experience, I know:

a. Data on the **Subject Devices** can provide evidence of a file that was once on the **Subject Devices** but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of

who used or controlled the device at a relevant time. Further, forensic evidence on a device can show how and when the device was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access, use, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the device user. Last, forensic evidence on a device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information on a device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a computer (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a

device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

Nature of Examination

29. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Subject Devices** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **Subject Devices** to human inspection in order to determine whether it is evidence described by the warrant.

30. The initial examination of the **Subject Devices** will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

31. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the **Subject Devices** do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

32. is search warrant does not require the search of physical items from PDX CODE GUILD. The electronic media on the **Subject Devices** to be searched was previously copied and imaged from the **Subject Devices** onto the Drive pursuant to a federal search warrant on December 7, 2022.

33. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

34. Based on the foregoing, I have probable cause to believe, and I do believe, that the **Subject Devices** described in Attachment A contain evidence of violations of 18 U.S.C. § 641 and 18 U.S.C. § 1343, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the **Subject Devices** described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

35. Prior to being submitted to the Court, this affidavit, the application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Andrew

Ho. I was informed that it is AUSA Ho's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

CHRISTOPHER MILLER
Special Agent
Department of Veterans Affairs,
Office of Inspector General

Sworn via telephone in accordance with the requirements of Fed. R. Crim. P. 4.1 at 12:17 pm am/pm on January 14, 2025.

Youlee Yim You

HONORABLE YOULEE YIM YOU
United States Magistrate Judge

DISTRICT OF OREGON, ss: AFFIDAVIT OF CHRISTOPHER MILLER

Affidavit in Support of an Application for a Search Warrant

I, Christopher Miller, being duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Department of Veterans Affairs ("VA"), Office of Inspector General ("OIG"). I have held this position since October 2014. I was previously a Special Agent with the U.S. Secret Service from July 2006 to October 2014. My current assignment is to the Northwest Field Office in the Portland, Oregon Resident Agency. My training and experience include criminal law and procedure training at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia and at the U.S. Secret Service Academy in Beltsville, Maryland.

2. Because this affidavit is being submitted for the limited purpose of securing authorization for a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that Sheri DOVER, owner/operator of PDX CODE GUILD, and others involved in the operation of PDX CODE GUILD, have committed and are committing violations of, among others, 18 U.S.C. § 641 (Theft of Government Funds) and 18 U.S.C. § 1343 (Wire Fraud). Furthermore, I believe that evidence, fruits, and instrumentalities of these violations, more particularly described in Attachment B to this affidavit (herein incorporated by reference), are presently located at the premises known as PDX CODE GUILD, located at 407 NE 12th Avenue, Portland, Oregon 97232 (referred to as the "**Subject Premises**"). The **Subject Premises** are more particularly described in Attachment A to this affidavit, which is incorporated by reference.

3. Based upon the investigation to date, I submit that there is probable cause to believe that the owner and operator of PDX CODE GUILD, Sheri DOVER, has executed and is executing a scheme to defraud the VA with respect to educational assistance payments for veterans of the United States Armed Forces and other eligible persons. PDX CODE GUILD and its owner and operator have, among other things, submitted false and fraudulent materials to the VA indicating that they are (1) charging the VA tuition for veterans within regulations not exceeding non-veteran students, and (2) composing courses with appropriate levels of supported and non-supported students (adhering to the 85-15 Rule).

4. Part I of this Affidavit outlines legal authority and jurisdiction. Part II describes the VA benefit programs that are being defrauded, as well as related statutes and regulations governing educational assistance to veterans and other eligible persons. Part III provides background information relating to the subjects of this investigation. Part IV sets forth the facts that support probable cause to search the **Subject Premises**. Part V describes specific information regarding the search and seizure of computer information. Part VI concludes.

Legal Authority and Jurisdiction

5. This Affidavit is made in support of an application for search warrant under Federal Rule of Criminal Procedure 41 to search the **Subject Premises** and any computer and storage medium found on the **Subject Premises**. The **Subject Premises** is in the District of Oregon, and thus, this Court has jurisdiction to issue the requested search warrant.

Target Offenses

6. I believe there is probable cause to believe that evidence of the following violations will be found in the places to be searched:

/ / /

- 18 U.S.C. § 641, Theft of Government Funds, provides in part:

> Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted— Shall be fined under this title or imprisoned not more than ten years, or both.

- 18 U.S.C. § 1343, Wire Fraud, provides in part:

> Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

Background on Veterans Affairs Educational Assistance

A. Educational Assistance Under the Post-9/11 GI Bill

7. Under Title 38, United States Code, Chapter 33 – the "Post-9/11 GI Bill" – the United States provides educational assistance by paying for tuition, housing costs, and other

educational costs and fees for veterans of the United States Armed Forces and other eligible persons that meet certain qualifications.[1] *See* 38 U.S.C. § 3311.

8. On October 1, 2011, the VA implemented a significant change in the eligibility for receipt of Post-9/11 GI Bill benefits. Effective that day, the VA began paying Post-9/11 GI Bill benefits to individuals pursuing non-institute of higher learning, non-degree programs, to include non-college degree ("NCD") schools or programs (such as a trade school). These benefits are commonly referred to as "Chapter 33 benefits."

9. For individuals receiving Chapter 33 benefits, the VA pays the tuition and fee payment directly to the school on the enrolled veteran's behalf.[2] The VA will cover the net costs for in-state tuition and fees or the annual maximum for the academic year, whichever is less for a NCD school. *See* 38 U.S.C. § 3313(g)(3). In addition to the tuition and fee payments, the VA will also provide monthly housing allowance benefits to veterans who are enrolled in the NCD program on more than a half-time basis. In addition, veterans enrolled in courses in a NCD program at a non-IHL school will receive a lump-sum amount for books, supplies, equipment, and other educational costs in an amount equal to $83 for each month (pro-rated based on the veteran's VA benefit level).

/ / /

/ / /

[1] The Post-9/11 GI Bill and its related regulations provides educational assistance to veterans and other eligible persons and is administered by the VA. Other statutes provide for education assistance to active-duty military service members; these programs are generally administered through the Department of Defense.

[2] In addition to veterans, other classes of individuals – including a veteran's spouse or child to whom the veteran has transferred his benefit entitlement – can be eligible to receive Post-9/11 GI Bill benefits. For purposes of clarity, I have used the term "veteran" to mean any person receiving Post-9/11 GI Bill or VET TEC benefits.

B. The Approval Process and Other Regulations Relating to the Receipt of Benefits Under the Post-9/11 GI Bill

10. To be eligible for benefits under the Post-9/11 GI Bill, a course of education must be approved "by the State approving agency ("SAA") for the State where the educational institution is located," subject to limited exceptions. 38 U.S.C. § 3672(a). In the state of Oregon, the SAA is the Oregon Higher Education Coordinating Commission ("OHECC").

11. Non-accredited institutions seeking approval from the SAA are evaluated in several areas to ensure that quality education is provided to veterans. For a school to obtain approval to offer a non-accredited course, the SAA must find upon investigation that the educational experience and qualifications of the school's instructors are adequate and that the instructors are of good reputation and character. 38 C.F.R. § 21.4254(c)(3), (c)(12). As a result, the school must disclose this information to the SAA during the approval process. *See* 38 C.F.R. § 21.4254(c)(3), (c)(12).

12. Non-accredited institutions seeking approval from the SAA must maintain a written record of previous education and training of the veteran which clearly indicates that appropriate credit has been given by the school for previous education and training, with the training period shortened proportionately. 38 C.F.R. § 21.4253(d)(3).

13. Once the school's course of education has been approved, tuition assistance under the Post-9/11 GI Bill is paid directly to the school providing the course in the amount allowable under the statute. *See* 38 C.F.R. § 21.9680(a)(1). Before assistance is paid out, however, the school must first certify the individual's enrollment in the approved program. *See* 38 C.F.R. § 21.9680(b)(1). Other benefits, including the housing allowance, funds for books and supplies, and other educational costs, are paid directly to the veteran. *See* 38 C.F.R. § 21.9680(a)(2).

14. Schools are not permitted to charge more for courses offered to veterans receiving benefits pursuant to the VA's educational benefit programs as compared to civilian applicants who do not receive such benefits. *See* 38 C.F.R. § 21.4210(d)(4)(i). If a school has overcharged a veteran or other eligible person, they may be disqualified from the benefit program altogether.

15. Moreover, the VA will not approve the enrollment of any veteran or other eligible person in any course for any period during which more than 85 percent of the students enrolled in the course are having any part of their tuition, fees, or other charges paid by the school or the VA. *See* 38 C.F.R. § 21.4201(a). That is, at least 15 percent of students must **not** be receiving any financial assistance—VA or otherwise. Failure to adhere to this requirement, which is commonly referred to as the "85-15 Rule," may result in the facility's future enrollments being suspended from receipt of VA educational assistance. *See* 38 C.F.R. § 21.4201(g)(2). In my experience, if an institution continually fails to abide by the 85-15 rule, it may be eventually wholly barred from receiving VA educational assistance.

C. Veteran Employment Through Technology Education Courses (VET TEC) Pilot Program

16. Under Public Law 115-48 – the "Harry W. Colmery Veterans Educational Assistance Act of 2017" – the VA provides educational assistance by paying for tuition and housing costs for a full-time high tech training program for veterans of the United States Armed Forces and other eligible person that meet certain qualifications. Generally, individuals that qualify for the VET TEC program must not be on active-duty or are within 180 days of separating from active duty; and qualify for VA education assistance under the GI Bill with at least one day of unexpired entitlement. If all these conditions are met and the veteran is accepted

/ / /

into a VA approved program, then the VET TEC training will not count against the veteran's GI Bill entitlement.

17. VA approved training providers enter into agreements with the VA to provide training and job placement outcomes. VA uses a “pay-for-performance" model that pays these institutions incrementally based on the progress and success of their students. The VA pays the training provider: an initial 25 percent of tuition and fees when the student enrolls and attends, another 25 percent when the student complete his or her training program, and the remaining 50 percent once the student secures meaningful employment in his or her field of student. The veteran must find employment within the field of study within 180 days of successfully completing the program in order for the VA to release the final tuition payment to the training provider. Documentation showing the student has found meaningful employment is required, which includes certification by both the veteran and the training provider that the veteran has achieved employment within the field of study.

18. Forms that must be completed by prospective training providers during the application phase include the VET TEC Training Provider Application, VET TEC Pilot Program Participation Agreement, VET TEC Training Provider Facility Programs Spreadsheet, and the VET TEC Statement of Compliance with 85-15 Ratios and Spreadsheet. Training providers with more than one site are also required to fill out a form identifying the names and locations of any additional training sites during the process.

19. The VA will give preference to training providers who agree to reimburse the VA for tuition paid when a veteran student successfully completes a program of education but does not find full-time meaningful employment within the 180-day period beginning on the date the student completes the program. If a training provider is approved with preference, they are

prioritized on the GI Bill webpage for approved VET TEC schools, are exempt from the 85-15 requirement, and are also exempt from the private school tuition and fees cap established by the VA during that fiscal year.

D. School Certifying Officials and VA Reporting Requirements

20. Each school in receipt of VA tuition assistance funds, including GI Bill and VET TEC, must designate a School Certifying Official (SCO) who is responsible for the certification of beneficiaries of VA education benefits. A school may designate more than one SCO. An individual in a position of authority at the school must complete VA Form 22-8794, Designation of Certifying Official(s), in order to designate an SCO. SCOs are required to submit initial enrollment documents for veterans within 30 days of the beginning of the term, keep the VA informed of the enrollment status of veterans, maintain current knowledge of the VA rules and benefits, maintain records of veteran and non-veteran students, and make all records available for inspection at any time by the VA or the SAA.[3]

21. VA-ONCE is a web-based system, with servers based in Pennsylvania, that allows SCOs to create and transfer enrollment information directly to a VA Regional Office for processing. The VA-ONCE system requires the School Certifying Official to provide a username and password to access the system and transmit data to the VA. Each SCO has a unique username and password which allows him or her access to the system.

22. SCOs must complete VA Form 22-1999, VA Enrollment Certification, for each veteran who will receive VA tuition assistance funds. Using this form, SCOs certify the course

/ / /

[3] In this affidavit, the term "non-veteran" is used to describe an individual student or enrollee who is not utilizing VA education benefits to pay for their program at PDX CODE GUILD.

in which the veteran is being enrolled, the start and end dates of the enrollment period, the number of hours per week the veteran will attend class, and the cost of tuition for the course. The SCO is responsible for notifying the VA of any changes in the information s/he has certified. In addition, if the student graduates from the program, the SCOs must document this graduation on VA Form 22-1999b, Notice of Change in Student Status. *See* Public Law 114 – 315 § 404.[4]

23. The SCO has the option of completing either a hard copy VA Form 22-1999 or the electronic version of the form available through the VA-ONCE system. The hard copy form requires the SCO to provide their signature, while the electronic form requires the SCO to provide an electronic signature. The date of the electronic signature and the date the document is electronically received by the VA are recorded on the enrollment certification document. By signing a VA Form 22-1999, either by hand or electronically, an SCO certifies that the veteran's course or courses are "generally acceptable to meet requirements for the student's educational, professional, or vocational objective," and that all the "85-15 ratio requirements have been satisfied."

24. The educational facility is responsible for ensuring that veterans receiving VA tuition assistance do not make up more than 85 percent of their student population. The VA does not track the number of non-veteran students, rather it relies solely on the representations made by the SCO on the Statement of Assurance of Compliance with 85 Percent Enrollment Ratios form, VA Forms 22-1999, and during VA compliance surveys, which are typically conducted on

/ / /

/ / /

[4] Public Law 114 – 315 § 404 became effective on January 1, 2018. Prior to this date, if there were no changes to the enrollment, there was no requirement for the SCO to submit any further documentation to the VA.

an annual basis. These representations are material to the VA, because a school that did not comply with the rules would be ineligible to receive funds under the program.

25. My review of VA records shows that between 2019 and 2022, Sheri DOVER, PDX CODE GUILD SCO, submitted approximately 546 VA Forms 22-1999 to certify that approximately 187 veterans enrolled in and attended PDX CODE GUILD courses via the VET TEC program.[5] The submitted VA Forms 22-1999s show the enrollment certifications were received electronically through the VA-ONCE system and signed electronically by Sheri DOVER and were transmitted by electronic communication in interstate commerce from Oregon to Pennsylvania.

26. A review of VA Forms 22-1999s submitted Sheri DOVER shows that between 2017 and 2022, Sheri DOVER, PDX CODE GUILD SCO, submitted approximately 240 VA Forms 22-1999 to certify that approximately 110 veterans enrolled in and attended PDX CODE GUILD courses via the Post 9/11 GI Bill program. The same records show that the enrollment certifications were (1) signed electronically by Sheri DOVER, (2) transmitted electronically to the VA-ONCE system from Oregon, and (3) were received electronically through the VA-ONCE system in Pennsylvania.

E. Retention of VA Records

27. Records including those pertaining to students not receiving benefits from the VA, as well as those pertaining to each period of enrollment of a veteran or other eligible person, should be retained at the school for at least three years following the termination of the

[5] Schools are required to submit enrollment certification forms for each course that a veteran is enrolled in, and veterans can take multiple courses. Also, a new enrollment certification form is submitted when a School Certifying Official needs to make a change to a current enrollment.

enrollment period. *See* 38 C.F.R. § 21.4209(f). Longer retention is not required unless a written request is received from the VA or the General Accountability Office. The law thus requires PDX CODE GUILD to maintain such records for recent years. As set forth below, there is probable cause to believe the records are located at the SUBJECT PREMISES.

Background on PDX CODE GUILD

28. A search of the Oregon Secretary of State's business registry showed PDX CODE GUILD LLC first registered in the State of Oregon on September 11, 2013; registry number 96368098. It registered as a Domestic Limited Liability Company and listed its registered agent and organizer as Sheri DOVER. An amendment to its Articles of Incorporation dated December 6, 2013, listed Sheri DOVER as its only member and owner. PDX CODE GUILD identified its business activity as an adult career school specializing in computer programmer bootcamp. PDX CODE GUILD's business registration is active and the 2021 filing listed its mailing address and primary place of business as 407 NE 12th Avenue, Portland, Oregon 97232.

29. PDX CODE GUILD course catalogs indicate that instruction is provided at one campus, 407 NE 12th Avenue, Portland, Oregon 97232. Bank records received and analyzed thus far reflect that the VA has deposited educational assistance funds for veterans attending PDX CODE GUILD into a Selco Community Credit Union bank account ending in 8108.[6] The most recent bank records reflect PDX CODE GUILD's address as 407 NE 12th Avenue, Portland, Oregon 97232. Sheri DOVER is the signatory on the 8108 Account.

30. Multnomah County property records for 407 NE 12th Avenue, Portland, Oregon show that the **Subject Premises** is part of a building complex which is currently owned by

6 Selco Community Credit Union is a credit union headquartered in Portland, Oregon. The PDX CODE GUILD bank account that received funds from the VA is located in Portland, Oregon.

"ELSEA FLOWER FARM LLC." The **Subject Premises** is part of 407-411 NE 12th Avenue which is an industrial/office building area totaling approximately 7,390 square feet. ELSEA FLOWER FARM LLC is owned by Sheri DOVER; she is also listed as the registered agent and organizer. According to property records that I reviewed, I believe that PDX CODE GUILD owner/operator Sheri DOVER rents the property located at 407 NE 12th Avenue, Portland, Oregon 97232 (**Subject Premises**) between her two different businesses.

31. Effective April 14, 2017, PDX CODE GUILD was approved by OHECC to receive VA tuition assistance funds under the Post-9/11 GI Bill for the purpose of providing education and training to eligible veterans and other eligible persons. According to VA records, DOVER submitted the initial application and subsequent recertification documents to OHECC and VA. VA recognized the school as a non-IHL, non-college degree facility providing information technology training to its students. From 2017 to present, PDX CODE GUILD has maintained certification to provide training to veterans and receive VA payments. The approval letter noted that the school will maintain a written record of the previous related education and training of veterans.

32. According to pertinent VA records, effective April 1, 2019, PDX CODE GUILD was first approved by VA to participate in the Veteran Employment Through Technology Education Courses (VET TEC) Pilot Program. The VA recognized the school qualified within the VET TEC program by providing information technology training in a non-degree program. Sheri DOVER signed PDX CODE GUILD's VET TEC Participation Agreement on May 1, 2019. In addition, PDX CODE GUILD's initial VET TEC Application, signed by DOVER on May 29, 2019, included a section titled "Statement of Understanding – 85-15 Rule." This section required a different signature from DOVER and explained that the VA would not

approve an enrollment in any program for any veteran for any period during which the requesting institution was out of compliance with the 85-15 Rule.

33. Based on my review of VA records, from 2019 to present, PDX CODE GUILD has maintained VET TEC certification to provide training to veterans and receive VA payments.

34. VA records reflect that between 2017 and 2022, approximately eight information technology courses at PDX CODE GUILD were approved by OHECC and the VA to allow the school to receive tuition assistance funds.

35. The course catalogs provided by PDX CODE GUILD to the VA and OHECC included descriptions of the courses, and costs associated. PDX CODE GUILD's tuition has steadily increased with each annual course catalog:

a. 2016-2017: 12 Week Python Based Developer Bootcamp $8,500;
16 Week Python Based Developer Bootcamp $8,500;

b. 2017-2018: 12 Week Python Based Developer Bootcamp $12,500;
16 Week Python Based Developer Bootcamp $12,500;

c. 2018-2019: 14 Week Python Based Developer Bootcamp $18,400;
16 Week Python Based Developer Bootcamp $16,500;
Node & React Full Stack Bootcamp $11,500;
Advanced Portfolio Bootcamp $10,500;

d. 2020-2021: 14 Week Python Based Developer Bootcamp $18,400;
18 Week Python Based Developer Bootcamp $17,600;
Node & React Full Stack Bootcamp $14,600;
Advanced Portfolio Bootcamp $17,500;

e. 2021-2022: Full-time Python Based Developer Bootcamp $21,400;

Evening Python Based Developer Bootcamp $19,600;

Advanced Node & React Full Stack Bootcamp $15,700;

Advanced Portfolio Bootcamp $17,500;

Advanced Full-Time Full-Stack Bootcamp $25,100;

Advanced Evening Full-Stack Program $24,000.

Statement of Probable Cause

A. Overview of the Fraud Scheme

36. The VA OIG is investigating PDX CODE GUILD's receipt of VA educational benefits through the Post-9/11 GI Bill and the VET TEC programs. As described in greater detail below, this investigation has revealed sufficient evidence to establish probable cause to believe that PDX CODE GUILD's principal, Sheri DOVER, and some employees are engaged in a scheme to fraudulently obtain education benefits paid by the United States on behalf of eligible veterans under VA programs, including Post-9/11 GI Bill and VET TEC.

37. PDX CODE GUILD initially obtained approval to receive VA education assistance benefits by representing to the VA, among other things, that it would follow VA regulations and its course catalogs which specified course tuition costs. PDX CODE GUILD agreed to adhere to course composition regulations, which dictate courses should not be overly dependent on veteran students, not to exceed 85 percent supported students, including veteran students. Upon enrollment, a PDX CODE GUILD SCO certified to the VA by way of VA Forms 22-1999 that course composition and tuition regulations were being met. As a result, PDX CODE GUILD then received direct tuition payments from the VA under the Post-9/11 GI Bill and VET TEC programs.

38. This investigation has included interviews of former students and employees, and review of bank records and VA records which revealed evidence that Sheri DOVER is providing false information to the VA concerning the: (1) tuition cost of PDX CODE GUILD courses included in its course catalogs and (2) composition of courses with respect to supported and non-supported students, including veteran students. As a result of the false information provided by Sheri DOVER, owner/operator, of PDX CODE GUILD and her employees, the VA has been and continues to pay VA education benefits to PDX CODE GUILD.

B. VA Funds Received by PDX CODE GUILD and Bank Account Activity

39. VA records indicate that from January 2017 to March 2022, VA has paid tuition assistance to PDX CODE GUILD totaling more than $3,300,000. Records show that 53% of these payments pertained to veterans who enrolled under the Post-9/11 GI Bill program and 40% were from the VET TEC program. In addition to the monies paid directly to PDX CODE GUILD by the VA, from 2017 to 2022, the VA has paid veteran students enrolled at PDX CODE GUILD under various VA education benefit programs approximately $4,993,099 in the form of housing allowances and stipends for books and supplies.

C. Interviews of Former PDX CODE GUILD Students and Employees

40. On September 8, 2022, federal agents employed with VA OIG conducted an interview of former PDX CODE GUILD student and employee John Fial. Fial worked as a teachers' assistant for instructor Merritt Lawrenson teaching the 14 week Python based bootcamp in approximately May 2021. The course consisted of approximately 12 to 13 students with only one paying non-veteran student, CJ Heideman. Heideman had a girlfriend and/or roommate named Brea Brown who also attended the course.

/ / /

41. Review of records showed the above-mentioned course had the following students:

NAME	COURSE DATES		STATUS	PAYMENT
Brea Brown	5/17/2021	8/28/2021	Non-Veteran	No record
Jeremy Bush	5/17/2021	8/28/2021	Veteran	18,400.00
Kelsey Canoy	5/17/2021	8/28/2021	Veteran	18,400.00
Ceth CJ Heideman	5/17/2021	8/28/2021	Non-Veteran	8,750.00
Austin Hennessey	5/17/2021	8/28/2021	Veteran	18,400.00
Jeremy Lamb	5/17/2021	8/28/2021	Veteran	18,400.00
Nicholas Fry	5/17/2021	8/28/2021	Non-Veteran	No record
Jonathan Spanning	5/17/2021	8/28/2021	Veteran	18,400.00
Ryan Woolsey	5/17/2021	8/28/2021	Veteran	18,400.00
Ross Zeiger	5/17/2021	8/28/2021	Veteran	18,400.00
Joseph Townsend	5/17/2021	8/28/2021	Veteran	18,400.00

42. Three non-veteran students were identified: Nicholas Fry, Brea Brown, and CJ Heideman. My investigation showed that no payment information was located for Nicholas Fry or Brea Brown. Two checks from Heideman which totaled approximately $8,750 were identified. Of note, two out of three non-veteran students did not pay tuition, and the third, Heideman, had a tuition cost that was well below the course catalog and his veteran classmates. My investigation showed that Heideman received disproportionate tuition decreases and financial support from PDX CODE GUILD versus the veteran students. As a result, PDX CODE GUILD had non-veteran, supported students and violated VA's 85-15 Rule.[7]

/ / /

/ / /

7 As explained paragraphs 15 and 23–24, supra, non-veteran, supported students do not count towards the "15" in the 85-15 rule.

43. On September 23, 2022, federal agents employed with VA OIG conducted an interview of former PDX CODE GUILD employee Lisa Nguyen. Nguyen stated when composing a course, DOVER foremost focused on veteran students. Nguyen also stated she would find non-veteran students to help meet the 85-15 Rule. To find non-veteran students, DOVER would: 1) find a non-veteran student that could pay course tuition, 2) offer a non-veteran student a scholarship to assist with tuition, and 3) placed PDX CODE GUILD staff into a course as students. PDX CODE GUILD staff did not pay tuition; during Nguyen's job interview DOVER stated employees attend courses for free.

44. For example, Nguyen herself attended the PDX CODE GUILD nighttime advanced course from approximately April 27, 2020, to July 18, 2020. Evan Hackett was the instructor. Nguyen was working at PDX CODE GUILD while attending the course and did not pay to attend the course. She was the only non-veteran in the course.

45. On September 20, 2022, federal agents employed with VA OIG conducted an interview of a former PDX CODE GUILD employee June Bremmer. Bremmer stated Sheri DOVER arranged all student tuition, registration, and course scheduling. DOVER also submitted all the paperwork to the VA.

46. In February 2021, DOVER told Bremmer her son, Scott Bremmer, could attend PDX CODE GUILD via an internship. DOVER proposed Scott would receive an "extreme discount" on tuition and a scholarship from an outside company. The company would cover some of the course cost. Ultimately, Scott attended the 14 Week Python Based Bootcamp for $3,000; the course started on April 4, 2021. DOVER told June, "I'm giving you a really good deal."

/ / /

47. On September 26, 2022, federal agents employed with VA OIG conducted an interview of former PDX CODE GUILD student Scott Bremmer, a non-veteran. Bremmer spoke with Sheri DOVER about attending a course sponsored via an internship with Zaelot, a private company. Zaelot was operated by a PDX CODE GUILD alum Jeff Lombard. Bremmer attended the PDX CODE GUILD 14 week Python Based Bootcamp starting on April 5, 2021. June Bremmer paid $3,000 for Scott to attend to the course. Scott Bremmer signed a contract with Zaelot for his internship and worked as a contract employee. Post course, Bremmer worked at Zaelot for one month at $25 per hour. Zaelot paid Bremmer's salary direct to PDX CODE GUILD to pay off the remainder of the cost of the course at $4,000. The total cost of the course was $7,000. Again, this tuition cost deviated significantly from the course catalog price and cost paid by the VA for veterans in that course (pursuant to PDX CODE GUILD's alleged compliance with the 85-15 rule).

48. On October 6, 2022, federal agents employed with VA OIG conducted an interview of a former PDX CODE GUILD employee, Lynn Nguyen (the sister of Lisa Nguyen). Lynn Nguyen started working at PDX CODE GUILD in September 2019. Nguyen tracked and submitted the number of veteran and non-veteran students in every course. She recalled VA's 85-15 Rule but did not recall any specifics. DOVER never instructed Nguyen on how to compute the 85-15 ratio or if students were supported vs. non-supported. Nguyen only identified students as veteran or non-veteran. She provided the lists to VA to satisfy the 85-15 Rule.

49. Regarding non-veteran students, Nguyen stated "we had a special discount for those." There were a number of discounts, including those for women and low income, and most non-veterans received a 50% tuition discount. Nguyen stated nearly every student other than "white men" and "veterans" received a discount. DOVER asked students to write a paragraph

explaining their situation, financial or otherwise, and she would grant them a discount. DOVER made the tuition discount decision on her own.

50. Nguyen surmised DOVER did not discount veterans' tuition in the VET TEC program because she knew she would likely not get the entire tuition payment because they required post course employment.

51. Nguyen attended the 18 Week Python-Based Evening Bootcamp from February 24, 2020, to July 3, 2020, for free while she was an employee. However, not all employees attended courses for free. She recalled two other non-veterans in the course, and they also had tuition discounts.

D. Non-veteran Student Records

52. An Inspector General Subpoena served on Southeast Works, a non-profit in Portland, OR, identified additional non-veteran students at PDX CODE GUILD. Southeast Works records showed it paid full and partial tuition for several students between 2017 and 2022 via a workforce training grant.

53. A Southeast Works payment of $6,000 on July 7, 2017, paid full tuition for Cynthia Prevatte to attend the daytime Full-Stack Python Based Developer Bootcamp from June 26, 2017, to September 20, 2017. Within the student file, PDX CODE GUILD noted its course price was $8,000. VA records showed no veteran supported students in the course.

54. A Southeast Work payment of $6,000 on October 3, 2017, paid full tuition for Jeffrey Bailey to attend the daytime Full-Stack Python Based Developer Bootcamp from August 23, 2017, to November 16, 2017. Of note, VA records show at least two veterans attended the above course and VA paid tuition to PDX CODE GUILD at $8,000 per student.

/ / /

55. A Southeast Works payment of $6,000 on January 1, 2018, paid full tuition for Emily Hall to attend the daytime Full-Stack Python Based Developer Bootcamp from November 27, 2017, to February 23, 2018. Within the file, it was noted the student was "awarded a diversity scholarship, and full cost of training is $8,000." VA records show one veteran, Ronnie Mosley, attended the above course and VA paid tuition to PDX CODE GUILD at $8,500.

56. A Southeast Works payment of $6,000 on February 23, 2018, paid full tuition for Anna Spysz to attend the daytime Full-Stack Python Based Developer Bootcamp from January 16, 2018, to April 9, 2018. VA records showed six VA supported students in the above-mentioned course; VA paid tuition of $8,000 for two veterans $12,500 for four veterans.

57. An Inspector General Subpoena served on Immigrant and Refugee Community Organization (IRCO), a non-profit in Portland, OR, identified additional non-veteran students at PDX CODE GUILD. IRCO records showed it paid tuition for several students between 2020 and 2022 via a workforce training grant.

58. An IRCO payment of $8,000 on January 12, 2022, paid tuition for Lujock Dhol to attend the daytime Full-Stack Developer Bootcamp from January 3, 2022, to April 15, 2022. VA records show nine veterans attended the course and VA paid $21,400 per veteran.

59. An IRCO payment of $6,500 on July 28, 2020, paid tuition for Haoua Dogo to attend the evening Full-Stack Developer Bootcamp from February 24, 2020, to July 3, 2020. VA records show five veterans attended the course and VA paid $16,500 per veteran.

60. The above tuition payments for non-veteran students show a continual pattern of lower tuition costs negotiated by PDX CODE GUILD. As a result, PDX CODE GUILD continually provided non-competitive tuition decreases for non-veterans which it financially

/ / /

supported. These students could not have been reported as non-veteran and non-supported in its 85-15 Rule adherence.

E. Review of PDX CODE GUILD Records

61. During a compliance survey, a copy of PDX CODE GUILD student and veteran Daniel Adams' student file was provided to VA. A review of the file showed Adams attended a PDX CODE GUILD course on April 27, 2020. PDX CODE GUILD previously reported its 85-15 Rule compliance to VA and listed 9 total students with 5 veterans and 4 non-veterans. The table below lists the students PDX CODE GUILD identified as attending:

NAME	COURSE DATES		STATUS	PAYMENT
Matthew Magnotta	4/27/2020	7/18/2020	Veteran	6,069.79
Austen Cote	4/27/2020	7/18/2020	Veteran	10,500.00
Lisa Nguyen	4/27/2020	7/18/2020	Non-Veteran	No record
Dustin DeShane	4/27/2020	7/18/2020	Veteran	7,500.00
Brandon Gonzalez	4/27/2020	7/18/2020	Veteran	10,500.00
Johnny Phompadith	4/27/2020	7/18/2020	Veteran	10,500.00
Daniel Adams	4/27/2020	7/18/2020	Veteran	10,500.00
Luke Hammer	4/27/2020	7/18/2020	Non-Veteran	No record

62. Of note, the student composition did not match that previously provided to VA; PDX CODE GUILD misrepresented the student composition which did not meet VA guidelines of 85-15. No payment information was located for several students, including Luke Hammer, and Lisa Nguyen. As noted above in Nguyen's interview, she did not pay for the course and was the only non-veteran. Again, since Nguyen was financially supported by PDX CODE GUILD she could not count as a non-veteran non-supported student.

63. During a compliance survey, a copy of PDX CODE GUILD non-veteran student Matthew Chimenti's student file was provided to VA. A review of the file showed Chimenti

attended a PDX CODE GUILD course on April 5, 2021. The table below lists the students PDX CODE GUILD identified as attending:

NAME	COURSE DATES		STATUS	PAYMENT
James Keicher	4/5/2021	6/25/2021	Veteran	11,500.00
Jo Omley	4/5/2021	6/25/2021	Veteran	11,500.00
Joseph Deveney	4/5/2021	6/25/2021	Veteran	7,500.00
Lisa Brown	4/5/2021	6/25/2021	Veteran	11,500.00
Matthew Chimenti	4/5/2021	6/25/2021	Non-Veteran	3,750.00
Stephen Johnston	4/5/2021	6/25/2021	Veteran	11,500.00
Zach McBride	4/5/2021	6/25/2021	Non-Veteran	No record

64. Of note, tuition payment for non-veteran student Matthew Chimenti was listed in his file at $7,500 because of an "income-based discount." However, in PDX CODE GUILD's financial records reflected only one payment from Chimenti in the amount of $3,750 on April 7, 2021. Since Chimenti was awarded an additional non-equal tuition discount he became "supported" by PDX CODE GUILD. As such, there were no identifiable non-veteran students who were not supported by PDX CODE GUILD, and this was most likely an additional violation of VA's 85-15 Rule.

65. In addition to the information reported during Compliance Surveys, a review of VA records, and PDX CODE GUILD's financial records revealed additional inconsistencies with tuition costs. For instance, PDX CODE GUILD's course on March 16, 2020, showed the following attendees:

/ / /

/ / /

NAME	COURSE DATES		STATUS	PAYMENT
Devan Fischer	3/16/2020	7/24/2020	Veteran	16,500.00
Eboni Washington	3/16/2020	7/24/2020	Veteran	16,500.00
Terrance Mitchell	3/16/2020	7/24/2020	Veteran	16,500.00
Manuel Trujillomaciel	3/16/2020	7/24/2020	Veteran	16,500.00
Brea Murakami	3/16/2020	7/24/2020	Non-Veteran	8,000.00

66. The tuition payment from the only identifiable non-veteran student, Brea Murakami, was $8,000, substantially less than veteran students at $16,500. Again, the non-veteran student received an extreme tuition discount and became financially "supported" by PDX CODE GUILD. As such, this was likely an additional violation of VA's 85-15 Rule.

Search and Seizure of Computers and Computer Storage Media

67. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **Subject Premises**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

68. I submit that if a computer or storage medium is found on the **Subject Premises**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when

files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

/ / /

/ / /

Electronic Records

69. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

70. There is probable cause to believe, and I do believe, that records will be stored on a digital device because, based on my knowledge, training, and experience, I know PDX CODE GUILD owner Sheri DOVER operates a school specializing in computer-based training. Additionally, based upon my review of VA record and interviews with former employees I know PDX CODE GUILD primarily uses digital devices to communicate and store business records.

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d. Based on actual inspection of other evidence related to this investigation, including education records, financial records, and invoices, I am aware that digital devices were used to generate, store, and print documents used in the education benefits fraud scheme. Thus, there is reason to believe that there is a digital device currently located on the Premises.

71. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the Premises, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file

(such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate

the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

72. In most cases, a thorough search of the Premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant.[8]

73. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital

/ / /

8 To clarify, I am not seeking to search the person of Sheri DOVER. I am seeking authority from the Court to seize digital devices found at the premises, and where necessary, will seek authority to unlock those devices using further legal process.

devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

Nature of Examination

74. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

75. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

76. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

77. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

78. If a computer or storage media contains evidence, fruits, contraband, or is an instrumentality of a crime, the government may retain that computer or storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

79. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

80. PDX CODE GUILD is a functioning company that conducts legitimate business. The seizure of PDX CODE GUILD's computers may limit PDX CODE GUILD's ability to

conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve investigating on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. At all times where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of PDX CODE GUILD so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the PDX CODE GUILD's legitimate business. If, after inspecting the computers, it is determined that some or all this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

Conclusion

81. Based on the foregoing, I have probable cause to believe, and I do believe, that Sheri DOVER, owner and primary operator of PDX CODE GUILD, and others are violating the Target Offenses in a scheme to defraud the VA. Specifically, there is probable cause to believe that DOVER submitted false information to the VA (over interstate wire from Oregon to Pennsylvania). The falsehoods included misrepresentations about: (1) course compositions by falsely understating the number of non-supported, non-veteran students (lack of adherence to 85-15 Rule) and, in turn, (2) the course tuition costs listed in PDX CODE GUILD course catalogs (by inflating the costs associated with course programs due to the discounts offered, but not disclosed, to non-veteran students). Essentially, DOVER implemented a scheme to defraud the VA by charging veteran students full tuition, as listed in the course catalogs provided to the VA, while disproportionately awarding non-veteran students discounts or scholarships to significantly decrease their tuition (versus veteran students). This caused large amounts of non-veteran

students to be financially supported by PDX CODE GUILD—students who would in actuality, if not for misrepresentations by DOVER, be viewed by the VA as "supported" students. Thus, PDX CODE GUILD continually violated the VA's 85-15 Rule, but continually certified otherwise.

82. As a result, DOVER received financial payments from VA to support her institution and unduly benefited from payments to which she was not entitled. I further submit that there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of the scheme to defraud will be located at PDX CODE GUILD. Based on the VA's records retention requirement and the statements above, there is probable cause to believe that records reflecting the accurate student course composition and course tuition costs to veteran and non-veterans will be located at the Subject Premises.

83. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Siddharth Dadhich. I was informed that it is AUSA Dadhich's opinion that the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

Request for Sealing

84. I further request that this Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrants, including the applications, this affidavit, the attachments, and the requested search warrants.[9] I believe that

9 On December 2, 2022, I incorrectly copied June Bremmer, former PDX CODE GUILD employee, on an email with an attached draft search warrant affidavit. I meant to email June Thomquist, a Legal Assistant at the United States Attorney's Office for the District of Oregon. After being alerted of this error by AUSA Dadhich, I immediately called Ms. Bremmer, and she

sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and any disclosure of the information at this time may result in flight from prosecution, the destruction of or tampering with evidence, and/or otherwise seriously jeopardize an investigation. Premature disclosure of the contents of the applications, this affidavit, the attachments, and the requested search warrants may adversely affect the integrity of the investigation.

By Phone IAW Fed. R. Crim. P. 4.1
CHRISTOPHER MILLER
Special Agent
Department of Veterans Affairs,
Office of Inspector General

Sworn to before me telephonically or by other reliable means pursuant to Fed. R. Crim. P. 4.1 at 2:20 p.m. on December 2, 2022.

HONORABLE ANDREW D. HALLMAN
United States Magistrate Judge

informed me that upon receipt, she had permanently deleted the email with the attachment. Ms. Bremmer noted she did not review the attachment and did not plan to discuss the matter with anyone as she knew it would negatively impact the investigation.

ATTACHMENT A

Property to Be Searched

The property to be searched are images of a MacBook Air (FVHY9DPTJ1WK), MacBook Pro (serial C02NV957G3QD), MacBook Pro (serial ND2K2H2WJH), MacBook Pro (serial NMVT7XK9XK), MacBook Pro (serial PWYWX2HJP9), HP Pavilion (serial SCG-10174YS), and iPhone 14 Pro (serial LJ6TH5L7) (collectively referred to as the Subject Devices) that are copied onto a Seagate Barracuda Drive (serial W1F54ND8) (the "Drive"), which is currently located at the VA OIG Portland, Oregon evidence vault located at 2121 SW 4th Avenue, Suite 301, Portland, Oregon 97201.[1]

[1] The Subject Devices loaded on the Drive were loaded onto evidence servers controlled by VA OIG. As part of this warrant, agents of VA OIG will search the Subject Devices as they were uploaded from the Drive onto the evidence servers.

ATTACHMENT B

Items to Be Seized

1. All records, data, and information on the Subject Devices described in Attachment A that relate to violations of 18 U.S.C. § 641 (Theft of Government Funds) and 18 U.S.C. § 1343 (Wire Fraud), including:

a. Any electronic/digital document, record, correspondence, or communication reflecting, referring to, or relating to ownership, dominion, or control of PDX CODE GUILD;

b. Electronic/digital Personnel and payroll files and records, such as employee lists, documents reflecting names, addresses, duration of employment, pay schedules, W-2s, 1099s, and duties of employees and independent contractors for PDX CODE GUILD;

c. Any electronic/digital document, notes, record, correspondence, or communication reflecting, referring to, or relating to the United States Department of Veterans Affairs ("VA") and any VA-related program, or the Oregon Higher Education Coordinating Commission ("OHECC");

d. Any electronic/digital document, notes, record, correspondence, communication, or item, of any nature, reflecting the names and identifying information of currently enrolled, formerly enrolled, or prospective students at PDX CODE GUILD, including student lists, class rosters, attendance sheets, grade lists, and student files;

e. Any electronic/digital document, photograph, notes, record, correspondence, or communication reflecting, referring to, or relating to veterans[1] currently enrolled at PDX CODE GUILD, formerly enrolled at PDX CODE GUILD, or seeking to enroll at PDX CODE GUILD;

f. Any electronic/digital document, photograph, notes, record, correspondence, or communication reflecting, referring to, or relating to any representation by PDX CODE GUILD or any of its officers, agents, employees, or contractors concerning or relating to the enrollment of veterans or non-veterans at PDX CODE GUILD, including, but not limited to, the ratio of enrolled veterans to non-veterans;

g. Any electronic/digital document, photograph, notes, record, correspondence, or communication reflecting, referring to, or relating to the amount, type, or quality of instruction provided by PDX CODE GUILD to any veteran;

h. Any electronic/digital document, photograph, notes, record, correspondence, or communication reflecting, referring to, or relating to the status of the education of any veteran enrolled as a student at PDX CODE GUILD, such as the veteran's performance in a class or whether a veteran successfully completed a class.

i. Any electronic/digital document, photograph, notes, record, correspondence, or communication reflecting, referring to, or relating to the method, means, or source of payment for the enrollment of any non-veteran;

---

[1] In this Attachment B, the term "veteran" means any person receiving VA educational benefits. Similarly, the term "non-veteran" means any individual student or enrollee who was not utilizing VA education benefits to pay for their program at PDX CODE GUILD.

j. Any electronic/digital document, record, communication, and item, of any nature, identifying offsite storage utilized by PDX CODE GUILD for veteran enrollee files;

k. Any electronic/digital document, record, communication, and item, of any nature, identifying other business locations used by PDX CODE GUILD for the training and education of veteran enrollees;

l. Any electronic/digital PDX CODE GUILD invoices related to services allegedly provided to veteran students;

m. Electronic/digital Bank records, wire receipts, wire transfer records, or any other document or item reflecting receipt, transfer, or use of funds from the VA;

n. Electronic/digital Financial records or documents relating to assets or accounts accessed by the owners and operators of PDX CODE GUILD that relate to payments from the VA;

o. Any electronic/digital document, photograph, notes, record, correspondence, or communication reflecting, referring to, or relating to a motive to devise, execute, or aid and abet a scheme to submit false or fraudulent representations to the VA concerning PDX CODE GUILD's services to veterans, or to submit false or fraudulent representations to the VA concerning PDX CODE GUILD's compliance with VA regulations;

p. Any electronic/digital document, photograph, notes, record, correspondence, or communication reflecting, referring to, or relating to the existence of a conspiracy to submit false or fraudulent representations to the VA concerning

PDX CODE GUILD's services to veterans, or to submit false or fraudulent representations to the VA concerning PDX CODE GUILD's compliance with VA regulations; and

q. Any electronic/digital document, photograph, notes, record, correspondence, or communication reflecting, referring to, or relating to any attempt to conceal a scheme to submit false or fraudulent representations to the VA concerning PDX CODE GUILD's services to veterans, or to submit false or fraudulent representations to the VA concerning PDX CODE GUILD's compliance with VA regulations.

2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

4. The examination of the Subject Devices may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Subject Devices to human inspection in order to determine whether it is evidence described by the warrant.

5. The initial examination of the Subject Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If

the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Subject Devices or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and it is determined that the Subject Devices do not contain any data falling within the ambit of the warrant, the government will return the Subject Devices to their owner within a reasonable period of time following the search and will seal any images of the Subject Devices, absent further authorization from the Court.

8. If the Subject Devices contain evidence, fruits, contraband, or are an instrumentality of a crime, the government may retain the Subject Devices as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Subject Devices and/or the data contained therein.

9. The government will retain forensic images of the Subject Devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to

questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third